AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The residence and premises at 1214 Applewood Drive, C107, Papillion, Sarpy County, Nebraska 68046
See Attachment B

Case No. 8:17MJ30

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
The residence and premises at 1214 Applewood Drive, C107, Papillion, Sarpy County, Nebraska 68046.
For further information, see Attachment B

located in the _____ District of Nebraska, there is now concealed *(identify the person or describe the property to be seized)*:
For further information, see Attachment A

SEALED

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C., Sections 2251, 2252, 2252A	Child pornography: transportation, production, receipt & distribution, possession;

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DET. BRANDON STIGGE, FBI-CETF-TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: 2-7-17

Judge's signature

City and state: Omaha, Nebraska

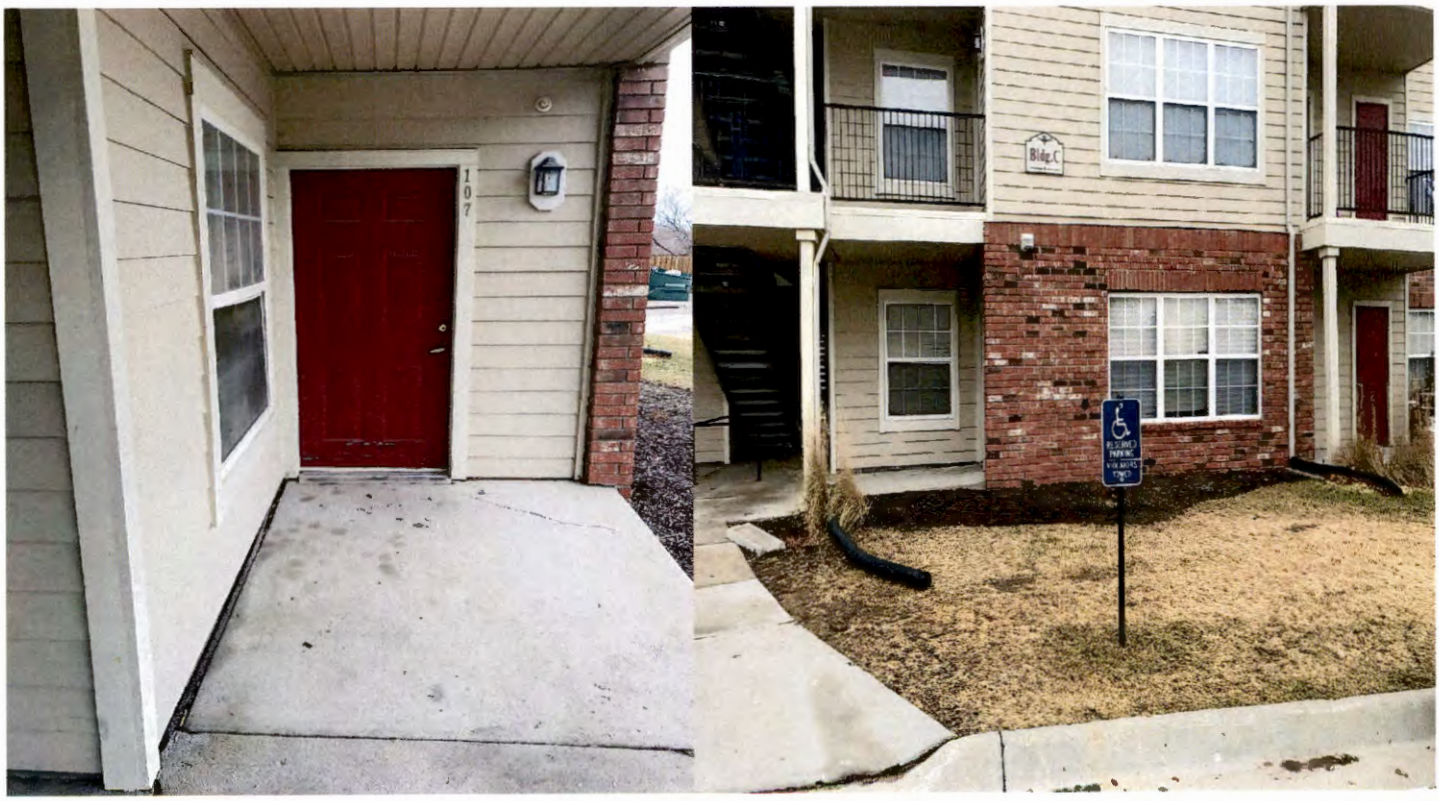
SUSAN M. BAZIS, U.S. Magistrate Judge
Printed name and title

ATTACHMENT B

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 1214 Applewood Drive, C107, Papillion, Sarpy County, NE is identified as follows:

1214 Applewood Drive, C107, Papillion, Sarpy County, NE is described as multi-family dwelling apartment building. The apartment is located on the ground level of the three-story complex on the north side of the building. The exterior door is red in color. The number "107" is displayed on a north trim board of the door frame. The legal description of the residence as reported by the Sarpy County Assessors Website is LOT 1 SUMMIT CLUB ADDITION



ATTACHMENT A
LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

> Any computer, computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, usb storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership and/or possession of the searched premises.

6. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

AFFIDAVIT OF OFFICER BRANDON STIGGE

I, Officer Brandon Stigge #469, having been first duly sworn, do hereby depose and state as follows:

1. I am a Police Officer with 10 years of experience in law enforcement with the Papillion Police Department. I am currently assigned to the Federal Bureau of Investigation (FBI) Child Exploitation Task Force (CETF) as a Federally Deputized Task Force Officer (TFO) in Omaha, Nebraska.

2. I have over sixty hours of training in Computer Forensics and over forty hours of training in child pornography. I also have attended training through the National White Collar Crime Institute, Cellebrite, Internet Crimes Against Children (ICAC), and the Federal Bureau of Investigations. I have a Bachelor's Degree in Criminal Justice. I have participated in several Peer-2-Peer investigations and at least fifty (50) child pornography investigations.

3. I make this affidavit in support of an application for a warrant to search the residence located at 1214 Applewood Drive C107, Papillion, Sarpy County, Nebraska 68046 which is more fully described in **Attachment B** of this affidavit.

4. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Police Officer in the Papillion Police Department. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Sections 2251, 2252, and 2252A exists at the residence.

I. COMPUTERS AND CHILD PORNOGRAPHY

5. I have assisted and participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. Investigators involved in this investigation have participated in various training hosted by the

National Center for Missing and Exploited Children (NCMEC), Internet Crimes Against Children (ICAC) Task Force training group, Federal Bureau of Investigations (FBI), and other law enforcement groups who addressed specific child pornography laws in which computers are used as the means for receiving, transmitting, manufacturing, and storing child pornography. Child pornography is defined in Title 18, United States Code, Section 2256.

6. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

7. The development of computers has changed this; computers serve five functions in connection with child pornography: production, communication, distribution, storage, and viewing.

8. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

10. The Internet and its World Wide Web protocol afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as applications service providers (Yahoo, MSN, Google) and Peer2Peer (Shareaza, Bearshare, Gnutella) groups among others. The online services allow a user to set up an account with a remote computing service that

provides e-mail services as well as electronic storage of computer files in a variety of formats. Programs also provide a similar nexus to share their files to millions of subscribers. Users can also set up online storage accounts from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software or other software used to obtain files of interest, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

13. A file transfer, upload, or download is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

II. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

14. Searches and seizures of evidence from computers commonly require investigators to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, computer related documentation, and peripherals) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto optical, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process

can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

III. SEARCH METHODOLOGY TO BE EMPLOYED

15. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to

appear in the evidence described in **Attachment A**; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment A.**

IV. DETAILS OF THE INVESTIGATION

16. On December 12, 2016, Officer Stigge received a report of possible possession of visual depiction of sexually explicit conduct, herein referred to as child pornography, occurring in Papillion, Nebraska.

17. Officer Stigge received CyberTip # 15234372 from Jessica Bowder of the Nebraska State Patrol. She reported that Dropbox, Inc. reported that a user, Justin Haynes, e-mail address whitefang76544@gmail.com and user ID 447771767, uploaded explicit files, presumed to be child pornography.

18. According to the NSP CyberTip, Dropbox, Inc. recorded whitefang76544@gmail.com uploading three (3) separate videos that contain erotic nudity and/or sexually explicit conduct of what visually appears to be female children. All three videos appeared to uploaded using the same account, with the same IP address 68.99.25.128. In addition, Dropbox provided an action log, which showed other files uploaded by the reported user. The action log revealed that other files with file names consistent with child pornography, including names with PTHC (Pre teen hard core) had also been uploaded. Those files had been uploaded with the same account name, but the IP address of 68.99.18.66

19. Dropbox traced the reported user back to IP addresses 68.99.18.66 and 68.99.25.128. Those IP addresses are assigned by Cox Communications. Dropbox, Inc. reported the user ID 447771767 logged on at these times and from these IP addresses:

68.99.25.128 Tue Oct 11 05:19:56 UTC 2016

68.99.25.128 Thu August 11 04:31:11 UTC 2016; and

68.99.18.66 Sun July 3 12:17:11 UTC 2016.

20. Affiant reviewed the videos that were uploaded to Dropbox from reported user ID 447771767.

a. The first video labeled "01.3gp"is a 35 second video of an apparent juvenile female. She is naked from the waist down and the camera is zoomed in on the vagina. There is a hand that is rubbing fingers back and forth on the vagina. The female

shown in the video is approximately 6 to 8 years old.

b. The second video is labeled "1b69cbe3-560d-40de-8ac7-a27820051b44.mp4". This video is 38 seconds long and is also of an apparent juvenile female. The female is naked from the waist down, and is standing. The female is placing an end of a blue hair comb in her vagina. The female also appears to discharge a clear fluid during masturbation with the comb. The female in the video is approximately 9 to 12 years old.

c. The third video is labeled "ac3458ff-21b2-4f6f-b9dc-2607ba6d073f.mp4". This video is one minute and thirty seconds. The video depicts two juvenile females entirely nude in a shower. The females are rubbing each other's genitals. At 20 seconds in the video one of the females is seen performing oral sex on the other. The end of the video depicts a female on a bed, nude, masturbating. The females depicted in the video are between the ages of 8 and 10 years old. BS SB (by me) BS SB (after I viewed them myself)

21. The files were confirmed to be child pornography as defined in Title 18, United States Code, Section 2256. Taken together, the above information indicates that on or before October 11, 2016, a person knowingly was in possession of child pornography in interstate and foreign commerce by means of a computer.

22. Dropbox, Inc. indicated that a member of their staff had reviewed the aforementioned files and determined the videos depicted children involved in sexual acts. A preservation letter was sent to Dropbox, Inc. on December 20, 2016. Dropbox Inc. assigned the case to an internal tracking number, CR-5000-2273

23. Dropbox, Inc. provided IP addresses of 68.99.18.66 and 68.99.25.128 These IP addresses currently are registered to Cox Communications.

24. Nebraska State Patrol Crime Analyst Jessica Bowder conducted a search for the whitefang76544@gmail.com , which yielded positive results linking that e-mail to Justin Haynes to include social media accounts with Twitter, Pinterest, and Facebook. Bowder also searched the Nebraska Criminal Justice Information System (NCJIS) which yielded positive result; Justin M Haynes (dob 1/3/86) at 1214 Applewood Drive, C107 Papillion, NE 68046.

25. On December 20, 2016, Officer Stigge queried a Nebraska Department of Motor Vehicles database for the name Justin Haynes, and located a person named Justin M Haynes, DOB 1/3/86, age

30. The address listed was 1214 Applewood Drive, C107, Papillion, NE, Sarpy, Nebraska. Additionally, Officer Stigge observed the Twitter page and Facebook page of Justin Haynes with e-mail linked whitefang76544@gmail.com. Stigge compared the photograph on the Facebook profile and Twitter of Justin Haynes to the photo on file with the Nebraska Department of Motor Vehicles. Officer Stigge determined the profile picture for Justin Haynes depicts Justin M Haynes DOB 1/3/1986.

26. On December 20, 2016, Officer Stigge served Dropbox, Inc. with a letter of preservation requesting Dropbox, Inc. to preserve all subscriber information and account contents for whitefang76544@gmail.com, User ID 447771767. Officer Stigge served Dropbox, Inc. with the preservation request via e-mail.

27. On January 4, 2017, Officer Brandon Stigge served Cox Communications with a Sarpy County Attorney subpoena requesting records and information relating to the identification of their subscriber using Internet Protocol (IP) addresses **68.99.25.128 Tue Oct 11 05:19:56 UTC 2016, 68.99.25.128 Thu August 11 04:31:11 UTC 2016, and 68.99.18.66 Sun July 3 12:17:11 UTC 2016**. These specific dates and times are when Dropbox, Inc. reported the apparent child pornography was uploaded from said IP addresses using whitefang76544@gmail.com, User ID 447771767 in CyberTip #15234372.

28. On January 30, 2017, Officer Stigge reviewed a responsive records form that Cox Communications provided. The requested records, which show that Internet Protocol (IP) addresses **68.99.25.128 and 68.99.18.66** were issued to Bonnie Rodr of 1214 Applewood Drive C107, Papillion, Sarpy County Nebraska, with the telephone number (402) 218-3743. Based on several dates of surveillance of 1214 Applewood C107, your Affiant has witnessed vehicles parked in the lot that are registered to Justin Haynes and Susan Masters. Both Susan and Justin also declared their residence as 1214 Applewood Drive C107, Papillion, NE Sarpy County, NE with the Nebraska Department of Motor Vehicles.

29. Cox Communications provided Internet Protocol (IP) lease records for their customer Bonnie Rodr, 1214 Applewood Dr C107, Papillion, Sarpy County, Nebraska, which showed that Bonnie Rodr was issued Internet Protocol (IP) address 68.99.18.66 since April 13, 2016, to July 28, 2016. For the specific dates and times aforementioned Dropbox, Inc. was accessed and videos had been uploaded as reported by Dropbox in CyberTip 15234372.

30. Additionally, Cox Communications provided Internet Protocol (IP) lease records for their customer Bonnie Rodr, 1214 Applewood Dr C107, Papillion, Sarpy County, Nebraska, which showed that Bonnie Rodr was issued Internet Protocol (IP) address 68.99.25.128 since July 28, 2016, to January 26, 2017. For the specific dates and times aforementioned Dropbox, Inc. was accessed and a video had been uploaded as reported by Dropbox in CyberTip 15234372

31. On January 9, 2017, at approximately 1600 hours, Officer Stigge was conducting surveillance at 1214 Applewood Drive C107, Papillion, Sarpy County, Nebraska and observed one vehicle registered to Justin Haynes. Officer Stigge observed a blue Ford Mustang with Nebraska license plate UFJ944. The car was parked in the south end of the parking lot.

32. On February 2, 2016, Officer Stigge met with Denise Hammer, property manager of Meridan Club Apartments located at 1214 Applewood Dr. She stated that the occupants registered to the apartment C107 are listed as Susan Masters, Bonnie Rodr, and Justin Haynes. She confirmed that Justin Haynes registered with their corporate office that he lives there 100% of the time.

33. Officer Stigge conducted a property search within the Sarpy County Assessor's website for 1214 Applewood Drive, Papillion, Nebraska, Sarpy County. The parcel reported a legal description listed as LOT 1 SUMMIT CLUB ADDITION

34. Your Affiant knows from training and experience that sometimes a person will keep data storage devices on their person. Many of these data storage devices are small enough to conceal easily in clothing, and can store hundreds or even thousands of files. Additionally, your Affiant knows from training and experience that oftentimes a person will transport computers and data storage devices in their vehicle.

35. Your Affiant knows from training and experience that searches and seizures of computer related evidence may require the seizure of most or all computer-related items (computer hardware, software, passwords and instructions) to be processed later by a qualified person in a laboratory, or other controlled environment. Computer hardware, which can be accessed by computers to store or retrieve data or images of child pornography, can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires analyzing authorities to examine all the stored data to determine whether it is included in the warrant. Due to time constraints, this sorting process renders it impractical to attempt

this kind of data analysis on site. Analyzing computers for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence, and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer related evidence is extremely vulnerable to tampering or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory may be required for its complete and accurate analysis. Affiant or other assisting Investigators may however conduct an examination of the computer hardware on-site using hardware and software that will not alter or change any potential evidence located on the computer hardware.

36. Your Affiant knows from training and experience that in order to fully retrieve files and data from computer hardware or a data storage device, the analyst may need the computer hardware as well as the data storage device. In cases like this one where the evidence consists partly of graphics files, input and output devices used for accessing computer data, and the associated computer data, may be required by an analyst to show the nature and quality of the graphic images, which the computer could produce. In addition, the analyst may need all the system software (operating systems or interfaces, and hardware drivers), and any application software, which may have been used to create the data (whether stored on internal or peripheral data storage devices), as well as documentation of the data, items containing or displaying passwords, access codes, usernames, or other identifiers necessary to examine or operate computer hardware, software, or files and data seized, or to activate specific computer hardware or software.

37. Your Affiant knows from training and experience that persons trading in, receiving, distributing, or possessing images involving the sexual exploitation of children or those interested in the sexual exploitation of children may communicate with others through correspondence or other documents (whether digital or written), which could tend to identify the origin of the images as well as provide evidence of a person's intent and interest in child pornography or child exploitation. Additionally, files related to the exploitation of children found on computer hardware are usually obtained from the Internet using application software, which often leaves files, logs, or file remnants, which would tend to show the exchange, transfer, distribution, possession, or origin of the files. Your Affiant is also aware from training and experience that computer hardware and software exists that allows persons to share Internet access over wired or wireless networks allowing multiple

persons to appear on the Internet from the same Internet Protocol address, and allowing mobility and concealment of the computer used to access the Internet. Examination of these items can reveal information about the authorized or unauthorized use of Internet connections.

38. Based upon your Affiant's knowledge, training, and experience investigating cases involving child exploitation and child pornography, your Affiant has learned and believes that contraband related to child exploitation and child pornography is typically collected, stored, and distributed by individuals with a sexual attraction to children that trade in this type of illegal activity. This type of contraband is not "used up" as other types of contraband can be such as alcohol or drugs. This type of contraband is usually stored in a manner that is secure but easily accessible to the persons collecting the contraband that is within their immediate control, to enable the collector to view their collection, which to them is highly valued, such as on computer hardware and data storage devices. For these reasons, contraband of this type can and is usually stored for an indefinite amount of time by the possessor, and may be found at the premises even though significant amount of time may have passed. In the experience and training of the Affiant, contraband stored in this manner has been found that was stored for years and transferred from and between computer hardware and data storage devices and from computer to computer where new computers are obtained by those who collect and trade in child pornography.

39. Collections can include books, magazines, diaries, letters, photographs, articles, newspapers, slides, movies, films, albums, digital images, drawings, audio tapes, video tapes, negatives, correspondence, mailing lists, child erotica, etc., and the equipment utilized to view or read any of these items.

40. Collections vary in size and in the items based on many factors. Factors, which can determine the size and extent of a collection, include living arrangements, economic status, and age.

41. The use of the computer has changed the collection of child exploitation material and individual behavior. Computers allow an individual to collect items and more easily hide their collection from others. The computer has in essence, allowed the individual who views or collects child pornography to maintain a certain anonymity via the Internet through the use of aliases known as "screen names" or "user names," as well as allowing for the storage of the collection and easy retrieval for viewing. The computer has also made it easy for individuals with similar behaviors to contact, exchange information and validate their behavior amongst each other. Computer hardware,

software, and related documentation are integral tools of this type of criminal activity and constitute the means of committing it. Given the information provided, individuals have the ability to view and store these types of items in their residence or a secure and easily accessible place, especially using computer hardware and or data storage devices.

V. CONCLUSION

42. Based upon the above information, I believe that probable cause exists to believe there has been a violation of Title 18, United States Code, Sections 2251, 2252, and 2252A, which prohibits possession, advertising, promoting, presenting, distributing, or soliciting through interstate or foreign commerce by any means, child pornography, and that evidence of those violations exist and are concealed on the premises known as 1214 Applewood Drive, C107, Papillion, Sarpy County, Nebraska, which is more fully described in **Attachment B** to this affidavit.

43. In consideration of the foregoing, I respectfully request that this court issue a daytime search warrant for the premises known as 1214 Applewood Drive, C107, Papillion, NE authorizing the search of the aforementioned premises for the items described in **Attachment A** and the seizure of such items for the purpose of searching and analyzing them.

44. Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Detective Brandon Stigge S-469, FBI-CETF-TFO
Police Officer, Papillion Police Department

Sworn to me on this 7 day of February, 2017.

SUSAN M. BAZIS
United States Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Nebraska

SEALED

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 8:17MJ30
The residence and premises at 1214 Applewood Drive, C107, Papillion, Sarpy County, Nebraska 68046 See Attachment B	)	

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nebraska
(identify the person or describe the property to be searched and give its location):

The residence and premises at 1214 Applewood Drive, C107, Papillion, Sarpy County, Nebraska 68046.

For further information, see Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A for additional details.

YOU ARE COMMANDED to execute this warrant on or before 2-14-17 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to SUSAN M. BAZIS.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2-7-17 at 9:30 a.m.

Susan M. Bazis
Judge's signature

City and state: Omaha, Nebraska

SUSAN M. BAZIS, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 8:17MJ30	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT B

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 1214 Applewood Drive, C107, Papillion, Sarpy County, NE is identified as follows:

1214 Applewood Drive, C107, Papillion, Sarpy County, NE is described as multi-family dwelling apartment building. The apartment is located on the ground level of the three-story complex on the north side of the building. The exterior door is red in color. The number "107" is displayed on a north trim board of the door frame. The legal description of the residence as reported by the Sarpy County Assessors Website is LOT 1 SUMMIT CLUB ADDITION

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

> Any computer, computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, usb storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership and/or possession of the searched premises.

6. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.